Minnesota Geospatial Advisory Council Meeting

September 28, 2022

11:00AM – 2:00PM

In-Person Option: Conference Room G13/14, Central Office Transportation Building,
Minnesota Department of Transportation, 395 John Ireland Blvd., St. Paul, MN 55155

Online Option: Via Microsoft Teams[1]

Agenda

1. Call to Order (Chair)	11:00	15 min
a. Introductions		
b. Approval of Agenda		
c. Approval of Meeting Minutes from May 25, 2022		
2. Review and Accept Committee Summaries (All) (p. 3-8)	11:15	10 min
3. Emergency Service Zone Data Standard (Carlson, Kotz)	11:25	5 min
4. Criminal Justice Information Best Practices update (Maddox) (p. 9-18)	11:30	10 min
5. PLSS Legislation update (Veraguth, Mavis)	11:40	5 min
6. 3D Geomatics Committee Update (Vaughn)	11:45	10 min
7. MN County GIS Association (MCGISA) (Maas)	11:55	10 min
8. Break & networking (no lunch on site, bring your own)	12:05	30 min
9. Sector Report – Hennepin County GIS (Albrecht)	12:35	10 min
10. NSGIC membership (Slaats)	12:45	5 min
11. Legislative Updates (Slaats)	12:50	10 min
12. Annual Priority Survey (Richter)	1:00	20 min
13. Updates on MN GAC Priority Projects and Initiatives (Richter)	1:20	25 min

[1] Contact MnGeo: gisinfo.mngeo@state.mn.us in advance for connection information

14. Announcements or Other Business	1:45	15 min
15. Adjourn	2:00	

Awards Committee

Report date:
September 15, 2022

Prepared by:
Len Kne and Phil Nagel (committee co-chairs)
lenkne@umn.edu and Phil.Nagel@bolton-menk.com

Meetings:

The Committee met two times (June 7 & August 1) this past quarter to review and recommend projects to receive the Governor's award. Met August 30 to review updates to the new Hub Site.

Progress on work plan:

1. Promotion of the applications for the Governor's Award has taken place on MN GIS/LIS and GovDelivery channels. Draft nomination packets were submitted by June 1, 2022 to allow the Committee to provide feedback for a strong submission; the intent is to get more nomination packets that meet the high standards of the Governor's Award. Final submissions were due June 30.

2. The Committee reviewed three applications for the Governor's Award.

3. Continue to work on content for new Hub site to encourage more applications to the Governor's Award. Thanks to Andra Mathews for leading this work.

Additional comments:

None.

Archiving Imagery Workgroup

Report date: September 21, 2022

Prepared by: Karen Majewicz (majew030@umn.edu), Melinda Kernik (kerni016@umn.edu)

Meetings:

- September 13, 2022: Interview with Brent Lund, MnGeo
- August 10, 2022: Interview with Jennifer Corcoran, MnDOT Resource Assessment and Tanya Mayer, Met Council (asynchronous interview conducted via documents)
- July 18, 2022: all members sharing research
- June 20, 2022: kickoff meeting

Progress on work plan:

- Made substantial progress on background research, including:
    - Researching historical and current formats of imagery data
    - Assessing the state of imagery in Minnesota (and the monetary investment involved in the original creation of Minnesota imagery) through conversations with state agency staff
- Submitted a poster proposal for the GIS/LIS conference
- Created a community survey to be shared during GIS/LIS conference
- Conducted three interviews with representatives from MnDOT, MnGeo, and the Metropolitan Council to learn more about their aerial imagery collections.

Next steps

- We will attend the GIS/LIS conference to present our poster
- We will work with GIS/LIS to distribute our community survey
- We are on track to complete a final report by the next GAC Quarterly meeting

CJIS Best Practices and Data Standards Guide for GIS

Report date: September 27, 2022
Prepared by: Britta Maddox

Meetings:
Second meeting – June 22nd, 2022
Third meeting – August 10th, 2022
Fourth meeting – September 21st, 2022

Chair: Britta Maddox, Business Analyst WCSO and GAC Member
Co-Chair: Cory Richter, Highway Supervisor for Ramsey County and GAC Member
Other team members attended as availability permitted

Progress on work plan:
Discussed scope and developed action items
Assigned action items to teammates and gathered initial information (May)
Assigned further action items and developed draft layout (June)
Reviewed initial draft layout and identified gaps (August)
Reviewed draft for presentation at GAC Meeting (September)

Additional meeting held between BCA and chairs of CJIS committee regarding purpose and scope of this document. Olivia Anderson from the BCA will be representing their interests on this committee moving forward and reviewing our documentation.

Additional comments:

- On the workgroup's webpage, see Meeting Minutes for June 2022, August 2022, September 2022
- CJIS Best Practices Guide DRAFT (note, work continues on layout and information) – see below in this agenda packet

Emergency Preparedness Committee

Report date: September 28, 2022

Prepared by:

- Chair: Stephen Swazee, Executive Director, SharedGeo, chair@mgacepc.org, 651-456-5411
- Vice Chair: Randy Knippel, GIS Manager, Dakota County, vchair@mgacepc.org, 952-891-7080

Full Committee/Leadership Team

Meetings:

- Full committee: None this quarter
- Leadership Team: None this quarter

Progress on work plan:

- Conduct at least three meetings of the full committee during 2022
  - No meetings to date due to Chair personal circumstances
- Conduct at least four meetings of the leadership team (Chair, Co-chair, and Project Team chairs)
  - No meetings to date due to Chair personal circumstances
- Continue efforts to cleanup committee's online presence and bring efficiency to its IT infrastructure
  - Ongoing – Gained Hub access and will be working to bring in current EPC website and expand functionality
- Randy Knippel to serve as EPC liaison to the Metropolitan Emergency Managers Association (MEMA) by attending that association's monthly meetings
  - Ongoing as defined above

Additional comments:

- Since inception in December 2020, MGAC EPC YouTube channel as had over 3,800 views: https://www.youtube.com/channel/UC3hwp5_9t3BkiTt-hyALArg/

Critical Infrastructure Assessment (CIA) Project Team – *GAC PRIORITY*

Stacey Stark, Associate Director, U Spatial, slstark@d.umn.edu, 218-726-7438

Meetings:

- Full Committee Meetings 1/14/22, 2/25/22, 3/16/22, 4/8/22, 7/1/22, 8/12/22, 9/23/22

- Law Enforcement dataset meeting: 3/15/22
- Related Partner Meetings: 2/4/22, 4/7/22
- Resource Site Meetings: 2/4/22

Progress on work plan:

- Conduct at least three meetings of the Project Team during 2022
  - Complete

- Develop updated data model (prioritizing fire and police) based on the previous standards identified in Minnesota Structures Collaborative project

    - Complete
- Publish comprehensive statewide dataset of police to the Minnesota Geospatial Commons
    - Complete: https://gisdata.mn.gov/dataset/struc-law-enforce-mn
- Pursue a long-term workflow to keep fire, law enforcement updated annually
    - In progress
- Request validation for 9 counties U-Spatial has projects with and remaining metro counties
    - In progress
- Maintain Esri online app for counties to validate their data (counties U-Spatial has other projects with, as a prototype for workflow)
    - On-going
- Develop workflow coordination with HSEM for fire, police, hospitals, schools.
    - On-going
- Continue to validate workflow with other partners
    - On-going
- Catalog available authoritative data sources
    - On-going
- Publish "C.I. resource site" on either MnGeo website or GAC Hub
    - Complete: https://www.mngeo.state.mn.us/chouse/criticalinfrastructure.html
- Develop strategy for outreach /promotion of work (use of GAC Hub)
    - Participation in GAC Hub subcommittee

Additional comments: Presentation at ESRI UC 7/14/22

Geospatial Assistance (GA) Project Team (Forming)
Brian Huberty, SharedGeo, bhuberty@sharedgeo.org, 651-706-6426

Meetings: None this quarter

Progress on work plan:
- Conduct at least three meetings of the Project Team during 2022
    - No progress this quarter
- Complete charter and work plan and receive approval from the EPC Leadership Team
    - No progress this quarter
- Develop first draft of procedures to help emergency managers understand steps for requesting aerial imagery and/or GIS support from federal, state and private assets
    - No progress this quarter

Additional comments: None

Underground Utilities Mapping (UUM) Project Team – *GAC PRIORITY*

Barbara Cederberg, CEO, Gopher State One Call (GSOC), barbara.cederberg@gopherstateonecall.org, 651-681-7303
Stephen Swazee, MGAC EPC, Chair, chair@mgacepc.org, 651-456-5411

Meetings:

- Leadership team: 1/21/22, 2/18/22, 3/25/22, 4/22/22, 5/20/22, 6/24/22, 7/22/22, 8/19/22, 9/23/22, next 10/14/22
- Large Group: 1/27/22, 2/24/22, 3/31/22, 4/28/22, 6/30/22, next 10/27/22

Progress on work plan:

- Conduct at least eight monthly meetings of the Project Team during 2022
  - Complete
- Produce a "Way Forward" blueprint document
  - On-going
- Complete development of a prototype system which can aggregate diverse utility geospatial data and make available for other project identified needs
  - Prototype functionally complete. GSOC preparing to contract for development of Open Source product to leverage concepts and approaches used during development of prototype.
- Deliver at least one presentation about overall team efforts at an established community appropriate conference (or webinar)
  - Complete – Multiple events this year to date. Next at MN GIS/LIS October 13-14.
- Publish at least one article about the Project Team in a publication of importance to the industry
  - Complete - Article featuring UUMPT Leadership Team member Geoff Zeiss of Ottawa, Canada was published in July issue of Damage Prevention-Pro.
- Continue efforts to develop project champions in the underground utility and regulatory communities
  - Statements of support: At their recent annual meeting, September 16, 2022, the Association of Minnesota Counties gave consideration to placing the UUMPT effort on their 2023 Platform.
  - Outreach Plan: During September 2022, initial promotional flyer was created and now in review. Dedicated support website (www.fuzionview.org) and outreach to the Minnesota utility community will commence in October.

Additional comments:

- Gopher State One Call COO Barbara Cederberg now working closely Common Ground Alliance GIS Working Group. The Minnesota project is seen as leading the nation and is receiving community wide support.

U.S. National Grid (USNG) Project Team – *GAC PRIORITY*

Randy Knippel, GIS Manager, Dakota County, Randy.Knippel@co.dakota.mn.us, 952-891-7080

Meetings:

- USNG Implementation Work Group: 3/16/22, 4/19/22, 5/17/22, 6/15/22, next 9/28/22

Progress on work plan:

- Conduct at least quarterly meetings of the USNG Implementation Working Group during 2022
  - 3/16/22, 4/19/22, 5/17/22, 6/15/22, next meeting 9/28/22
- Develop documentation for production of 10K maps
  - No progress this quarter
- As appropriate, publish or assist other government entities with publication of USNG maps for their areas of responsibility
  - No activity this quarter
- Refine, update, and publish Minnesota statewide 1K maps
  - No progress this quarter
- Work with SharedGeo to complete a new USNG mapbook publishing application on USNG Center (www.usngcenter.org)
  - Development complete. Anticipate release before end of year.
- Continue development of USNG training videos focused on USNG map production
  - This effort to be developed going forward in conjunction with other members of the national USNG Implementation Work Group
  - SharedGeo has reworked its WLIA virtual conference booth into a more generic booth featuring USNG information (www.sharedgeobooth.org)
- Conduct workshops and presentations where appropriate
  - Scheduled for two presentations at upcoming MN GIS/LIS Conference, October 13-14

Additional comments:

- USNGI has its own tax-deductible webpage at: https://www.givemn.org/story/Usngi
- Created proof of concept interactive map linking to all USGS US Topo maps, which are USNG compliant: https://www.arcgis.com/apps/webappviewer/index.html?id=126687ab78c247b9b5f21b2ffa367410
- Current development application for displaying USNG maps that are available anywhere in the United States: https://usng-form.herokuapp.com/map.

Standards Committee

Report date:
September 14, 2022

Prepared by:
Mark Kotz, Chair (mark.kotz@metc.state.mn.us)
Curt Carlson, Vice Chair (curtis.carlson@state.mn.us)

Meetings in 2022:
1/19/22 Stream ID standard subgroup
2/8/22 Standards Committee
2/14/22 Emergency Service Zone standard subgroup
2/22/22 Stream ID standard subgroup
4/1/22 Standards Committee meeting
9/13/22 eVote for ESZ Data Standard
10/19/22 Standards Committee

Full committee Meeting minutes available here

Progress on work plan:

1. Review draft Emergency Service Zone Data Standard for adoption by the GAC
   a. Initial draft of standard was presented to committee 2/8/22
   b. SME subgroup reviewed comments from Standards Committee and made revisions 2/14/22. Revised draft submitted back to Standards Committee
   c. Draft approved by standards committee 4/1/22 and published for public review period ending 7/31/22
   d. SME subgroup created draft responses to all public review comments and recommended minor changes to the standard 9/2/22.
   e. Committee eVote concluded to approve comments and changes to standard Responses to comments and 9/14/22
   f. Presenting revised standard to GAC for approval 9/28/22.
2. Review draft Stream ID standard for adoption by the GAC (this is a revision of a former GCGI standard)
   a. SME group reviewed and modified standard at meetings on 1/19 and 2/22. Revised standard to be submitted to Standards Committee
   b. Draft approved by standards committee 4/1/22 and published for public review period ending 7/31/22
   c. SME subgroup created draft responses to all public review comments and recommended minor changes to the standard 8/22/22.

    d. Revised standard and responses to comments will be presented to the Standards Committee for approval 10/19/22.

3. Review Stormwater Data Standard for adoption or endorsement by the GAC

    a. MetroGIS Stormwater standard presented to Standards Committee 2/8/22

4. Updating standards workflow to more deliberately announce/promote newly approved standards

5. Work with stakeholder groups to modify remaining original Governor's Council on Geographic Information (GCGI) standards to the GAC format and have adopted by the GAC. This will involve review and possibly changes to these standards.

    a. Minnesota Geographic Metadata Guidelines

    b. Codes for Identifying Watersheds

    c. Codes for Identifying Lakes and Wetland Basins

6. Facilitate the creation of usage guides for key GAC standards as time and resources permit.

MN Geospatial Advisory Council

Workgroup Members:

Chair – Britta Maddox, WCSO Business Analyst and MNGAC Member at-large
Co-Chair – Cory Richter, Ramsey Co Highway Supervisor and MNGAC Member

Trish Heitman-Ochs, Woodbury PD Crime Analyst
Matt Goodman, St Louis County GIS
Doug Matzek, Washington County GIS
Carey Strouse, Coon Rapids PD Crime Analyst
Karen Haines, WCSO Systems Manager
Karie Weldon, WCSO Business Analyst
Linda Curtis, WCSO Business Analyst
Olivia Anderson, BCA
Angela Backer-Hines, Eagan Crime Analyst
Garith Sherk, Minnetonka Crime Analyst
Eric Kopras, Woodbury GIS
Matt McGuire, MetCouncil

Mission Statement:

To provide best practices based on CJIS information sharing rules for connecting law enforcement and other CJIS regulated data to GIS systems for analysis and sharing

Objectives:

Discern CJIS-compliant best practices for sharing data within the GIS community, particularly as it relates to Emergency Management or critical incidents and infrastructure

Share this guide amongst the broader MN GIS community and use these principles to inform future MN GAC projects

Glossary of Terms:

- **MN BCA** - The Bureau of Criminal Apprehension (BCA) provides investigative and specialized law enforcement services to prevent and solve crimes in partnership with law enforcement, public safety and criminal justice agencies. Services include criminal justice training and development, forensic laboratory analysis, criminal histories and investigations.[2]
- **Criminal Justice Information (CJI)** - protected under the FBI's Criminal Justice Information Services (CJIS) Division's CJIS Security Policy which discusses authorized use, access, dissemination, and disclosure. See Appendix A for a copy of the CJIS Security Policy.
- **PII: Personally Identifiable Information** – in the scope of CJIS this includes any information that can be used to distinguish and trace and individual's identity. Examples include name, social security number, or other biometric records alone and or in conjunction with information such as DOB, place of birth, mother's maiden name, etc. This information must be extracted from CJI for official business only.
- **Safe at Home Act -** MN Statutes Chapter 5B, "The legislature finds that individuals attempting to escape from actual or threatened domestic violence, sexual assault, or harassment or stalking frequently establish new addresses in order to prevent their assailants or probable assailants from finding them. The purpose of this chapter is to enable state and local agencies to respond to requests for data without disclosing the location of a victim of domestic violence, sexual assault, or harassment or stalking; to enable interagency cooperation with the secretary of state in providing address confidentiality for victims of domestic violence, sexual assault, or harassment or stalking; and to enable program participants to use an address designated by the secretary of state as a substitute mailing address for all purposes."[3]
- **LASO: Local Agency Security Officer –** local agency contact ensuring hardware, software, firmware, and other technology-related programs meet CJIS policies and securely connect to state and federal systems with appropriate encryption and authorized access requirements. Often, this is the IT director for the local PD or Sheriff's Office.
- **TAC / Assistant TAC: Terminal Agency Coordinator –** local agency POC for CJIS access and compliance with CJIS policies. Often, this is the records supervisor or other office administrator for the local PD or Sheriff's Office.

[2] https://dps.mn.gov/divisions/bca/about/Pages/default.aspx

[3] https://www.sos.state.mn.us/safe-at-home/about-safe-at-home/

- **Critical Incidents –** As described by FEMA, "Any natural or man-made event, civil disturbance, or any other occurrence of unusual or severe nature that threatens to cause or causes the loss of life or injury to citizens and/or severe damage to property."[4]
- **Storage requirements for security** – where on the network, who can access, etc, what is 'public accessibility', password requirements/policy for access

Target Audience:

- **Data practices responsible authority within each agency –** this could include the TAC, alternate TAC, LASO, law enforcement staff who authorize and release response data (typically records staff or office administrators but can also be sworn peace officers).
- **IT technical requirements –** these are enumerated in the CJIS security policy and include requirements for network and physical security of devices used to store and view CJI. IT staff at each local agency should be versed in these rules and have adequate plans in place for ensuring network and physical security even in the event of a critical incident where the establishment of an EOC outside of normal physically secure buildings may be required.
- **Variations based on public-facing or internal LE-use only –** when referring to the CJIS security policy and MN statute 13.82 for the release of data, the qualifications only apply to the general public and parties named in the response or investigative data requested. All information, with minimal exception, can be shared between law enforcement entities without restriction provided transmission of the data is encrypted and the information is pertinent and necessary to the requesting agency in initiating, furthering, or completing an investigation.[5]

Training Requirements for Access:

- **CJIS Security Awareness Training and Test** – for anyone with potential access to CJI
  - Highly recommended for anyone who may access CJI during the course of their duties – including IT Staff responsible for network security and GIS Staff that may be called in during a critical incident
  - CJIS Online is located at https://www.cjisonline.com/
    - For a username and password, please contact your agency's Terminal Agency Coordinator (TAC).
  - Level 1 Security Awareness Training 5.2.1.1: Those with physical access only. These individuals are not performing a criminal justice function. They would have incidental access; i.e. janitorial, maintenance, vending machine vendors, etc.
  - Level 2 Security Awareness Training 5.2.1.2: Those with physical access only performing a criminal justice function; i.e. paper shredding, records clerks, scanning services, couriers, etc.
  - Level 3 Security Awareness Training 5.2.1.3: Those with physical and logical access. This access includes the electronic ability to see criminal justice information; i.e. majority of criminal justice staff, terminal operators, officers with MDTs, etc.
  - Level 4 Security Awareness Training 5.2.1.4: All those with an Information Technology role; i.e. system administrators, security administrators, network administrators, etc.
  - Certification valid for 2 years and then must be renewed

[4] https://training.fema.gov/programs/emischool/el361toolkit/glossary.htm

[5] https://www.revisor.mn.gov/statutes/cite/13.82#stat.13.82.21
Subd. 24

- BCA Training – specialized training courses for those fulfilling certain roles and general overview of data practices and CJDN operations
  - **TAC Workshop:** This one-day course is designed for new and existing Terminal Agency Coordinators (TAC) as a summary of the duties and responsibilities a TAC has with regard to BCA MNJIS and FBI NCIC access. By the conclusion of this class, students will have the knowledge and skill set for performing TAC functions at their agency.

    LEARNING OBJECTIVES

    Upon completion, the attendee will be able to:

    Describe CJDN policies and procedures
    Manage user accounts and certifications
    Obtain and analyze criminal history information
    Manage hot file records
    Describe the audit process and expectations

    AUDIENCE

    Terminal Agency Coordinators

    REGISTRATION: $25

  - **MNJIS Operator:** This two-day course, which combines the MNJIS One-Day Basic Operator course with additional specialized training, is designed for full-access operators who run queries and enter records into the Minnesota and NCIC hot files. Students completing this course will learn the policies and procedures for Criminal Justice Data communications Network (CJDN) operators. Students will gain an understanding of system security, file queries, criminal history, hot files, and the hit confirmation process. *This course covers the content from MNJIS One-Day Basic Operator.*

    LEARNING OBJECTIVES

    Upon completion, the attendee will be able to:

    Describe CJDN policies and procedures
    Process administrative messages
    Process KOPS messages
    Obtain and analyze criminal history information
    Query vehicle and registration information
    Classify and process hot file records
    Recognize identity theft
    Process vehicle files
    Process vehicle and boat part files
    Process boat files
    Process article files
    Analyze gun files
    Process missing person files
    Process wanted person files
    Obtain training resources

    AUDIENCE

    New or experienced operators who have full-access hot file entry and query job duties. It is recommended that students have direct access exposure to Portals prior to attending the class.

    REGISTRATION: $50

  - **LASO Certification** - located within CJIS Online.

  - As the LASO, you are required to complete both the Security Awareness and LASO certifications.

- Other training/certification/authorization may be necessary based on types of data

Authoritative Sources:

I. CJI – Only information coming from FBI CJIS Systems

Covered by CJIS Security Policy – very small scope
See Appendix A
Summary of the CJIS Security Policy – Designed to provide a minimum set of security requirements for creation, viewing, modification, transmission, dissemination, storage, and destruction of FBI-provided Criminal Justice Information (CJI). Agencies may impose stricter controls governing in a risk-based approach.

Section 3 of the CJIS Security Policy covers the roles and responsibilities that fall under each role within an organization when it comes to data security.

Section 4 defines CJI as the "…term used to refer to all of the FBI CJIS provided data necessary for law enforcement and civil agencies to perform their missions including but not limited to biometric, identity history, biographic, property, and case/incident history data."[6] Criminal History Record Information (CHRI) is a restricted subset of CJI data which is governed by CFR Title 28, Part 20 (Appendix D). Section 4 continues to discuss the proper access, use, storage, and dissemination of all the defined data that qualifies as CJI. Personally Identifiable Information (PII) is also defined here as that which can be used to distinguish and or trace an individual's identity, which is again protected by policy.

Section 5 describes the policy items and implementation steps of said policies that agencies must address. There are 13 policy areas – Information Exchange Agreements, Security Awareness Training, Incident Response, Auditing and Accountability, Access Control, Identification and Authentication, Configuration Management, Media Protection, Physical Protection, Systems and Communications Protection and Information Integrity, Formal Audits, Personnel Security, and Mobile Devices. These areas are covered in depth within the CJIS Security Policy, along with appendices that provide samples, diagrams, and best practices.

II. BCA-provided Data

Covered by CJDN Security policy
See Appendix B
Summary of the CJDN Security Policy – This document is intended to be an extension of the FBI CJIS Security Policy in reference to BCA-provided data, providing specific guidance for meeting CJIS Security requirements. The first portion of the document enumerates the difference between the CJIS System Agency Information Security Officer (CSA ISO), a BCA employee, and the Local Agency Security Officer (LASO). Enforcement and security are also listed here, providing that all agencies be responsible for ensuring appropriate measures are taken. The CJDN policy also provides standards for incident response, should there be a security breach, and a template for response policy, NIST Special Publication 800-61.

[6] CJIS Security Policy, page 10

Technical security standards make up the bulk of the CJDN security policy including account administration, advanced authentication, application development, BCA systems and data access, camera guidance for body/squad/surveillance cameras, cloud security, audio and video conferencing, employees, vendors and contractors, encryption, digital faxing, firewalls, logging, multifunction devices and printers, radio traffic, soft phones, VPNs, virtualization, vulnerability remediation and system updates, and wireless networks.

One of the main items in the CJDN Security Policy is the encryption requirements. All devices must be FIPS 140-2 compliant with a 128-bit symmetric key to access and or transmit CJI. In addition, when CJDN must be accessed outside of a physically secure location, advanced authentication must be used with the encryption to ensure data security. This is a particularly relevant consideration in times of critical incident management as temporary command posts may be established.

III. MN Chapter 13 – and data from other local agencies

See Appendix C
Summary of MN Statute 13.82 COMPREHENSIVE LAW ENFORCEMENT DATA[7]

> Disclaimer – there are many nuances to this statute and exceptions enumerated in other related statutes. Below is a basic summation of arrest, call for service, and incident response data and its default dissemination status. The statute itself should be viewed in its entirety prior to dissemination of any CJI and related statutes also

Whether or not data is public is partially dependent on its origination – Arrest data, Incident data, or Call for Service data.

Arrest data relates to any actions taken by law enforcement to cite, arrest, incarcerate, or otherwise substantially deprive an adult of liberty and shall be PUBLIC at all times. Booking photos taken at the time of arrest are also considered PUBLIC information. Data from arrest warrants is CONFIDENTIAL until the defendant is taken into custody, served, or appears before the court with exception for when making the information public would serve public interests.

Call for Service data relates to the request by the public for LE services is PUBLIC. The audio recording of a 911 call is PRIVATE except for a written transcript of the recording is PUBLIC, without revealing the identity of the caller.

Incident data is the documentation of law enforcement's response to the request for service as well as their actions taken under their own initiative for public safety and traffic incidents and is inherently PUBLIC.

Incident data regarding the investigation of a crime is deemed CONFIDENTIAL or PROTECTED NONPUBLIC until:

- a decision by the agency or appropriate prosecutorial authority not to pursue the case;

[7] https://www.revisor.mn.gov/statutes/cite/13.82

- expiration of the time to bring a charge or file a complaint under the applicable statute of limitations, or 30 years after the commission of the offense, whichever comes earliest; or
- exhaustion of or expiration of all rights of appeal by a person convicted on the basis of the investigative data.

After one of those clauses occurs, the information becomes PUBLIC upon request, unless the release of data would jeopardize other ongoing investigations and/or would reveal the identity of protected individuals. Any investigative data presented as evidence in court shall be public. A court order can also be obtained during an active investigation to release the contents of an investigation per judge's order. Public data may also be withheld if the agency reasonably believes that public access would endanger the physical safety of an individual or cause a perpetrator to flee, evade detection, and or destroy evidence. Any dispute of this withholding would need to be contested in court.

Reporters and victims of child abuse or neglect and reporters and victims of vulnerable adult maltreatment are always PRIVATE, whether active or inactive. Financial transaction data and account numbers are always PRIVATE NONPUBLIC, regardless of the investigation status. Data uniquely describing lost, stolen, recovered, or confiscated physical property is PRIVATE.

Investigative techniques and other law enforcement processes are considered CONFIDENTIAL provided they are publicly accepted practices under courts of law. However, the use of surveillance technology to capture audio, video, photos, or other electronic recording devises of the general public for purposes of conducting an investigation, responding to an incident or request for service, monitoring or maintaining public order and safety, or engaging in any other law enforcement function authorized by law is PUBLIC data.

This statute allows for discretion by law enforcement entities to make confidential or protected nonpublic data public when it is determined that the access will aid the law enforcement process, promote public safety, or dispel widespread rumor or unrest. There are also provisions for making public data inaccessible when not feasible to separate the public and nonpublic data and or when protecting the identity of certain individuals, as listed in the statute.

Common Tools and Best Use Cases:

These are only some tools available for use and most can be customized to a department's needs and security level. Below are some examples of available options and a brief synopsis of what that tool provides:

Open source/free mapping tools (Bing, Google, QGIS, etc.) – Review the platform's security standards and consider what data you are submitting to the service to be processed and/or stored in their cloud.

ArcGIS Pro Crime Analysis and Safety Toolbar – Set of crime analysis tools and sample projects that can be added to ArcGIS Pro to support tactical, strategic, and investigative analysis functions. Desktop tool, no CJIS/CJDN security concerns.

ArcGIS Pro Intelligence – A specific iteration of ArcGIS Pro directed at investigative and intelligence professionals. Still includes most of the normal ArcGIS tools, built to streamline intelligence data processing from multiple sources into visualizations (timelines and link charts integrated with maps). Desktop tool, no CJIS/CJDN security concerns.

ArcGIS Online and Story Maps – Online interactive maps and data dashboards for publishing and sharing data, internal or external. CJIS/CJDN security concerns depending on the data used in the applications and if it is stored in Enterprise Portal or ArcGIS Online (ArcGIS Online Cloud pending FedRAMP Moderate certification which is the equivalent of CJIS compliance).

Survey123 – Form-centric data gathering and sharing solution through a Mobile Application using ArcGIS. Shared feature services work hand-in-hand with Field Maps. Best use for collecting form data, such as surveys with pre-defined fields, can capture images, etc. CJIS/CJDN security concerns depending on the data used in the applications and if it is stored in Enterprise Portal or ArcGIS Online.

Field Maps – Map-centric data collection and sharing solution through a Mobile Application on devices with GPS capability to edit and track data through ArcGIS. Could be used to track graffiti, damaged utilities, managing fleet/equipment, etc. CJIS/CJDN security concerns depending on the data used in the applications and if it is stored in Enterprise Portal or ArcGIS Online

ArcGIS Mission – Built for command staff to streamline tactical operations during events, including planning, resource assignment and real-time updates and communication. Desktop and mobile application, track and visualize staff movements and sent information back and forth. Potential for CJIS/CJDN security concerns for officer safety and the data shared in the messaging component.

Drone2Map – Provides real-time or historic drone imagery which can be monitored live or turned into a 3D model of the location. Could be used to prepare for a search warrant, event planning, searching for missing persons, etc. Probably no CJIS/CJDN security concerns.

Transparency Hub/Crime mapping (public) – Pre-built customizable set of online story maps and dashboards supplied by ESRI to share public safety data with the public. CJIS/CJDN security concerns if data released through these tools is not public.

CrimeView Analytics

LexisNexis/Accurint – software itself is already compliant with security policies, based on what the BCA allows us to contribute. Secure access requirements and dissemination rules would apply.

GIS Data Sources:

Many GIS data sets that are useful for conducting crime analysis are publicly available for download. Below is a list of web resources where you may find some of the basic GIS layers you may need to conduct your work. Please note that care must be taken, following the guidance within this document, Minnesota statutes, and CJIS best practices, to ensure that combining these data with crime incident information does not violate an individual's right privacy (for example, tying a domestic abuse crime record to a parcel owner's name based on location and address).

Minnesota Geospatial Commons - a good place to find geocoding data sets like addressed road centerlines and address points.

Site: https://gisdata.mn.gov/

Minnesota Natural Resources Atlas - clearinghouse for Minnesota data mostly sourced from other entities

Site: https://mnatlas.org/

HIFLD (Homeland Infrastructure Foundation-Level Data) - clearinghouse for critical infrastructure data that is sourced from a wide variety of entities and systems. These data are not always authoritative or current, so it should be reviewed before use, but it is often still considered the 'best available'.

Site: https://hifld-geoplatform.opendata.arcgis.com/

Esri Living Atlas – data layers available to users within their ArcGIS Online system and include a vast array of curated data sets, including ready-to-use community demographic data, which helps put crime statistics into context.

Site: https://www.arcgis.com/ (requires a user account)

Minnesota NG9-1-1 Data - In support of the state's eventual transition from E9-1-1 to NG9-1-1, stakeholders are working towards aggregated statewide datasets for address points, road centerlines, and emergency services (fire, law, medical, etc.) boundaries. Those involved in this work are hopeful that these data sets can be made publicly available.

Address points, center lines, responder boundries – statewide coverage

MN BCA Crime Data Explorer – provides summary incident and arrest statistics statewide. Already compliant as it is provided publicly by the BCA. Jurisdiction-based, no latitude/longitude.

Appendix A: CJIS Security Policy

Appendix B: CJDN Security Policy

Appendix C: MN 13.82 Statute

Appendix D: CFR Title 28 Part 20